BancaFinanza
Mensile
Ketchum
Data 01-2013
Pagina 61/65
Foglio 1 / 5



Tecnologia & Informatica

CONTINUITÀ OPERATIVA LE NUOVE SFIDE

# Ripristino in sicurezza

In caso di disastri naturali, gli istituti di credito mettono in atto i piani di business continuity. E utilizzano il change management per le release che non funzionano.

■ ALBERTO MAZZA

Per i responsabili della sicurezza, della business continuity e del change management, il periodo prenatalizio si è rivelato decisamente critico, se non drammatico. No, niente Maya, niente fine del mondo e niente *millennium bug* a scoppio ritardato. A colpire sono stati, più semplicemente, due fenomeni provenienti dal cyberspazio, che hanno fatto vacillare le sicurezze dei consumatori. Il primo ha riguardato proprio il mondo bancario: si tratta di *Eurograbber*, malware devastante (partito, tra l'altro, dall'Italia) mirato alla violazione dei conti correnti on line; il virus, in modo simile a un attacco di phishing, ha colpito i computer e gli smartphone, permettendo ai pirati informatici di prelevare un totale di 36 milioni di euro da oltre 30.000 conti correnti. Secondo evento: il clamoroso disservizio di Trenord, che ha quasi paralizzato il traffico ferroviario in Lombardia, causando gravi disagi per alcuni giorni (a causare il blocco sarebbe stata una presunta incompatibilità del software *GoalRail*, già in uso alle ferrovie francesi - anche se, su internet, qualcuno nutre dubbi su questa versione).

Se Eurograbber dovrà spingere le banche a ripensare e rafforzare la sicurezza degli accessi (e gli utenti a raddoppiare la prudenza on line), il caos-Trenord sembra preoccupare meno gli istituti di credito. Perché, ci ha rivelato un "uomo di macchina" dell'informatica bancaria, «una società ferroviaria deve far viaggiare i treni: l'informatica è solo un accessorio per raggiungere questo obiettivo. Per una banca, invece, la gestione della sicurezza e del change management fa parte a pieno titolo del core business». «Nel caso Trenord», approfondisce **Giulio Piazzi**, della direzione governance Ict del Credito Valtellinese, «non è bastato avere qualche treno di scorta da poter utilizzare in sostituzione oppure un percorso alternativo da seguire: sarebbe stato necessario anche disporre di una modalità alternativa per organizzare la turnazione e l'assegnazione dei macchinisti alle vetture. Tuttavia può darsi che il problema sia stato più articolato. Per questo motivo, si rivela utile la conduzione di una *business impact analisys* che, pur realizzata a posteriori, costituirebbe la base per la definizione di un piano di continuità operativa da applicare in analoghe e possibili future situazioni di crisi».

## INTERRUZIONI DI SERVIZIO

Ma come agiscono le banche in casi simili? «Riguardo alla tematica delle interruzioni di servizio legate a problemi dovuti a malfunzionamenti del software, il gruppo Montepaschi provvede in "modalità reattiva" a fornire la continuità dei suoi processi produttivi attraverso l'applicazione di piani di business continuity o disaster recovery, con l'attivazione legata alla tipologia di problema riscontrato», dice **Marcello Milano**, responsabile dell'area sicurezza del consorzio operativo del gruppo Montepaschi. «Il gruppo, tuttavia, provvede in "modalità proattiva" a mitigare il rischio attraverso l'applicazione del processo di change management, che garantisce che l'ambiente di produzione riceva solo i cambiamenti, sia di tipo hardware, sia di tipo software, accuratamente testati e considerati affidabili attraverso l'applicazione di metodologie di verifica *ad hoc*».

«In ogni caso», aggiunge **Dario Bonavitacola**, responsabile delle infrastrutture tecnologiche e della si-

**VIA DI FUGA**
**Le banche prevedono una strategia di change management, per garantire che, nel caso in cui un nuovo software crei problemi, i sistemi It possano tornare alla versione precedente.**

# Tecnologia & Informatica

**TEST ACCURATI**
**«L'applicazione del processo di change management, garantisce che l'ambiente di produzione riceva solo i cambiamenti, sia di tipo hardware che software, accuratamente testati e considerati affidabili», sostiene Marcello Milano, responsabile dell'area sicurezza del consorzio operativo del gruppo Montepaschi».**

curezza di Cedacri, «la disaster recovery non ha nulla a ha che fare con eventi che si collocano con il normale sviluppo dei sistemi come il passaggio a una nuova release software, che è quanto è successo a Trenord. Quanto si è verificato non si sarebbe potuto evitare con un disaster recovery. Il modo per evitare che aggiornamenti del sistema informativo portino a problemi come questo è applicare strettamente una metodologia di sviluppo e controllo qualità nel software, che implica molti test prima del passaggio e garantisce in questo senso. E, qualora dovessero comunque verificarsi problemi a seguito della migrazione o dell'aggiornamento software, occorre avere tutte le contromisure per tornare indietro». Ciò che, alla fine, ha fatto Trenord. Troppo tardi, però.

**DUE PARAMETRI**
**«Il piano di business continuity si basa su due parametri: l'indicazione del tempo necessario per il pieno recupero dell'attività e il tempo massimo tollerabile che consente di contenere la gravità dell'impatto», dice Giulio Piazzi, della direzione governance Ict del Credito Valtellinese.**

## GOVERNO DELLA SICUREZZA

Ma torniamo alla business continuity. Che, per Montepaschi, è un'attività che si situa nella più ampia attività del governo della sicurezza. «Il governo della sicurezza riguarda argomenti e processi di alto livello», dice Milano, «come, in particolare, la definizione delle strategie e delle politiche di sicurezza, l'analisi e la gestione dei rischi, la continuità del business, la verifica dei livelli di sicurezza aziendale e il reporting direzionale. La sicurezza operativa», prosegue Milano, «coinvolge l'organizzazione aziendale, il personale e tutti i processi dedicati al mantenimento dei livelli di sicurezza in relazione a tre requisiti fondamentali: confidenzialità, integrità e disponibilità delle informazioni e delle risorse aziendali. In questo ambito sono gestiti aspetti come la sicurezza fisica e ambientale, la sicurezza del personale, la gestione degli incidenti di sicurezza, la gestione delle contingenze e il recupero da interruzioni di servizio e disastri, la configurazione e la manutenzione dei sistemi, nonché la formazione e la diffusione della consapevolezza sui temi di sicurezza aziendale. La sicurezza informatica, infine, riguarda specifici aspetti di controllo accessi, identificazione e autenticazione degli utenti, la tracciatura e il non ripudio delle operazioni eseguite, fino alla protezione dei sistemi, delle applicazioni e delle telecomunicazioni».

**PIANO DI CONTINUITÀ** Creval ha organizzato la sua struttura di business continuity management con un documento che viene aggiornato nel tempo, in considerazione dei continui cambiamenti che avvengono nel sistema Ict e nelle dotazioni tecnologiche. «Questo compito spetta al servizio business continuity e compliance», dice Piazzi, «che conduce regolarmente, con frequenze definite, l'attività di riesame della problematica. Il suo obiettivo è mantenere aggiornata la metodologia, per consentire una revisione periodica degli scenari di criticità e del perimetro dei processi critici, evidenziandone i rischi e individuando le aree di miglioramento e di mitigazione». Gli obiettivi del business continuity plan, prosegue Piazzi, «si concretizzano mediante la stima dei due parametri fondamentali: *recovery time objectives*, che indica il tempo necessario per il pieno recupero dell'operatività del servizio di business, e *maximum tolerable downtime*, che, per ogni processo, indica il tempo massimo tollerabile che consente di contenere la gravità dell'impatto. Quanto indicato potrebbe sembrare più teorico che pratico: in effetti, nel gruppo Credito Valtellinese, è strutturato anche un *business continuity plan*, per consentire alla banca di affrontare le conseguenze di un evento imprevisto, con potenziali impatti elevati. L'obiettivo è garantire il ripristino dei processi aziendali critici in tempi e modalità tollerabili e nel rispetto dei termini di servizio di business. Le modalità operative da seguire in caso di crisi o emergenza non fanno riferimento soltanto alla potenziale indisponibilità del sistema informativo o dei suoi componenti, ma anche alle indisponibilità fisiche degli uffici, delle persone o di altri elementi importanti per l'erogazione dei servizi agli utenti. Bankadati servizi informatici, che nel gruppo Credito Valtellinese ha la responsabilità per lo sviluppo e gestione del sistema informativo, è direttamente responsabile del *disaster recovery plan*». ■






Cedacri

BancaFinanza
Mensile
Ketchum
Data 01-2013
Pagina 61/65
Foglio 3 / 5



CONTINUITÀ OPERATIVA L'ESPERIENZA DI BANCA MARCHE

# «Così evitiamo le interruzioni»

L'istituto di credito ha installato il nuovo front end di filiale. Ecco come ha assicurato la prosecuzione del lavoro in caso di problemi in fase di deployment.

■ ALBERTO MAZZA

Quando una banca cambia dotazioni informatiche, la fase di roll out è sempre preceduta da un lungo periodo di test che precede la fase di deployment. Qui, si decidono eventuali correzioni di rotta, si risolvono le incompatibilità e si decidono le patch per eliminare i problemi che si possono incontrare quotidianamente. Ma, nonostante i test e i controtest che vengono effettuati, durante il roll out si possono verificare intoppi di vario tipo. «Se non accadesse proprio nulla, ci sarebbe da preoccuparsi», sorride **Paolo Branchesi**, responsabile area governo Ict di Banca Marche. Sta, naturalmente, al *change management* predisporre, in caso di problemi, il ritorno provvisorio ai vecchi sistemi nel più breve tempo possibile. Proprio in questi giorni, l'istituto con sede ad Ancona sta effettuando il passaggio dalle vecchie videate a caratteri a un nuovo front end di filiale. Branchesi e **Lamberto Spadari**, responsabile del nucleo che presidia la rete, i sistemi dipartimentali e la gestione dei sistemi di sicurezza di Banca Marche, ci spiegano come sta avvenendo e come sono stati superati i problemi quotidiani dovuti al deployment.

**Domanda. Come vi cautelate dagli inconvenienti che possono verificarsi in fase di cambiamenti informatici?**

**Branchesi.** Da anni abbiamo un sistema di change management, che ha il compito di permetterci il ritorno alle versioni precedenti dei software, se la nuova *release* non assicura la funzionalità precedente. Questo è il minimo che si possa fare: siamo attivi da un decennio sul mainframe, e da quasi due anni a questa parte siamo operativi anche sul mondo applicativo distribuito. Quando, dopo l'installazione di una nuova release, si è verificato un evento che non si era visto in collaudo, siamo tornati alla versione precedente in 15 minuti. Senza danneggiare le filiali.

**D. Capita di frequente?**

**Branchesi.** Una volta ogni tanto. Per esempio, è successo in dicembre: nell'avviare una nuova release del nuovo front end di filiale. Nel corso del roll out, abbiamo introdotto una *patch* per risolvere alcuni problemi. Nel passaggio in produzione, è emerso un problema non rilevato in collaudo. Quindi siamo tornati indietro alla vecchia versione e abbiamo riavviato la fase di test per quel software. Intanto, il lavoro per le filiali è proseguito: le dipendenze hanno avvertito un disservizio molto contenuto.


**D. A proposito: come sta andando il nuovo front end di filiale?**

**Spadari.** La fase di sviluppo sta volgendo al termine.

**D. Come è strutturata la soluzione?**

**Spadari.** Nasce da un disegno architetturale completamente nuovo; la tecnologia di base, fornita da Microsoft, è basata su uno smart client, tutto in .Net 4.0, e prevede l'introduzione dei workflow. Si passa da un'applicazione *keyboard-based* con videata a caratteri, a un'applicazione integrata con strumenti mouse. La nuova applicazione a sportello vuole essere un nuovo contenitore, con l'intento di facilitare l'operatività dello sportellista, e l'introduzione dei workflow è uno di questi. Non è solo una questione infrastrutturale, ma vuole risolvere il problema della stratificazione che si era accumulata in tutti questi anni.

**D. Da quanto lavoravate con la vecchia applicazione?**

**Branchesi.** Da 15 anni (anche se veniva utilizzata solo per la componente *core*, mentre diversi software a contorno erano già sviluppati via web). La vecchia ap-

**RITIRATA STRATEGICA**

**«Lo scorso dicembre, mentre stavamo avviando una nuova release del front end di filiale, abbiamo introdotto una patch per risolvere alcuni problemi», spiega Paolo Branchesi, responsabile area di governo Ict di Banca Marche. «Nel passaggio in produzione, è emerso un problema non rilevato in collaudo. Quindi siamo tornati indietro alla vecchia versione, e abbiamo riavviato la fase di test per quel software. Intanto, il lavoro per le filiali è proseguito: le dipendenze hanno avvertito un disservizio**

# Tecnologia & Informatica

**FRONT END**
«La vecchia applicazione di sportello presentava molte stratificazioni presenti nel tempo», spiega Lamberto Spadari, responsabile del nucleo che presidia rete, sistemi dipartimentali e gestione dei sistemi di sicurezza di Banca Marche. «Il nuovo front end di filiale ha, invece, l'obiettivo di mettere ordine e guidare l'operatore».

plicazione di sportello era arrivata al massimo livello di maturità: era tecnologicamente superata e non permetteva più estensioni funzionali. Insomma: adesso che era quasi perfetta, la dismettiamo.

**D. Che cosa cambia per lo sportellista?**

**Spadari.** Cambia sicuramente l'aspetto di «guida al lavoro» che le applicazioni di sportello possono mettere in funzione. La vecchia applicazione era frammentata, presentava molte stratificazioni presenti nel tempo. Quella nuova ha, invece, l'obiettivo di mettere ordine e guidare l'operatore. La nuova interfaccia è decisamente più intuitiva: permette, quindi, di acquisire confidenza in breve tempo.

**Branchesi.** Certamente, gli under 45 si sono adattati in una giornata. I colleghi meno giovani ci hanno messo un po' di più, perché erano abituati ai sistemi a carattere. Ma alla fine ce l'hanno fatta senza particolari problemi.

**D. Parliamo della business continuity in senso stretto.**

**Branchesi.** Per quanto riguarda la parte infrastrutturale, garantita sia in mainframe, sia per le parti distribuite, siamo in *outsourcing facility management* con Ibm. Il servizio comprende un sito per la disaster recovery, per riprendere l'operatività nel caso in cui si verificasse un «evento primario» (cioè un disastro, naturale o di altro tipo). Si prevede la replica asincrona dei dati: quindi, in caso di disastro, il sistema di *recovery* riparte dal punto di aggiornamento che era già stato allineato in precedenza.

**D. Parliamo dei tempi di ripristino...**

**Branchesi.** Prevediamo 12 ore per la ripartenza dell'attività, un tempo che è garantito contrattualmente. Per la perdita dei dati, invece, dai test che effettuiamo con cadenza annuale abbiamo registrato perdite insignificanti, sempre inferiori ai 60 secondi. Unico rischio calcolato può essere la perdita di qualche dato «in volo». Abbiamo anche una terza copia dei dati, che vengono portati su nastro in un ulteriore data centre a molti chilometri di distanza dal sito primario e da quello secondario. Il terzo sito ha il compito di attivarsi nel caso in cui, per qualche ragione, anche la struttura secondaria non possa partire. Abbiamo tutti i dati in un caveau, è vero, ma in questo caso la ripartenza sarebbe più lunga.

**D. Che differenza c'è tra il sito secondario e la terza copia?**

**Branchesi.** Che nel sito secondario sono pronti sia dati, sia macchine, mentre nel terzo sono disponibili solo i dati.

**D. Questo accade per le infrastrutture. Che cosa succede, invece, per la continuità operativa a livello di strutture aziendali?**

**Branchesi.** La aggiorniamo al nostro interno. La nostra direzione generale è organizzata su tre sedi fisiche: Jesi, Pesaro e Macerata. Se in una di queste strutture si verifica un problema tale da minare l'operativita sulla rete locale, questa può essere riattivata accedendo al nostro sito di business continuity, dove giornalmente sono attivati tutti i dati della rete locale: in una giornata, le strutture della banca possono riprendere l'operatività. Tutti gli anni vengono organizzati test per verificare l'efficacia della nostra business continuity. Sia quella infrastrutturale, sia quella interna. ■

**CONTINUITÀ OPERATIVA** IL PIANO DI EMERGENZA DELLA BPER

# Una rapida ripresa dopo il sisma

In seguito al terremoto, l'operatività bancaria è stata trasferita a postazioni mobili. E ora è tornata alle filiali. In questo modo.

■ FRANCO MARELLI

Banca popolare dell'Emilia Romagna è stata costretta a verificare il suo piano di business continuity e disaster recovery lo scorso maggio, in occasione del terremoto che ha colpito la Pianura Padana. In che modo sono stati assicurati i servizi bancari nelle aree coinvolte dal sisma? In quanto tempo sono stati riattivati dati e strutture della banca dopo le scosse? Ci sono stati problemi nel recupero di informazioni sensibili o nel loro utilizzo? Ce ne ha parlato **Marco Bertazzoni**, vicedirettore generale di Bper Services.

**Domanda. La vostra banca è stata pesantemente coinvolta nel terremoto dell'Emilia. Quali danni sono stati causati dal sisma? E in quanto tempo siete ripartiti?**

**Risposta.** Come sa, le scosse di grande rilevanza sono state due. Al momento del primo sisma, che è avvenuto il 20 maggio, sono state coinvolte sette nostre filiali. In particolare, abbiamo riportato danni importanti al punto di Modena Terminal, per il crollo di una sala di sta-


gionatura. Abbiamo ripristinato l'operatività di tutte le filiali nel giro di una settimana.

**D. Ma, pochi giorni dopo, è arrivato il secondo sisma, quello di 5,8 gradi della scala Richter...**

**R.** Sì. Ed è stata proprio la seconda scossa a provocare i danni più gravi. Alle 9 del 29 maggio (cioè meno di mezz'ora dopo la scossa, *ndr*) abbiamo riunito il team d'emergenza e convocato il comitato di crisi, con la presenza del nostro amministratore delegato. Poi abbiamo deciso di chiudere tutte le filiali vicine all'epicentro nel raggio di 20 chilometri.

**D. Quante succursali avete chiuso?**

**R.** Ne abbiamo chiuse 30, completamente. Abbiamo poi convocato due tipologie di risorse: i direttori di filiale e i responsabili dei processi critici. Di lì abbiamo studiato le mosse da attuare. Le riunioni hanno portato ad azioni immediate, come la conferma dell'evacuazione di 20 filiali delle 30 impattate e la predisposizione di opportune informazioni ai media e ai clienti tramite il nostro sito internet.

**D. Avete spostato l'operatività delle filiali chiuse in altre strutture non colpite dal terremoto?**


**R.** Sì. In pratica, abbiamo effettuato un appoggio su altre dipendenze con postazioni alternative. La predisposizione di strutture temporanee è stata immediata. Nel dettaglio, la banca ha alllestito otto camper, sette Atm mobili e cinque container per le filiali più critiche (quelle di Cavezzo, Concordia, Crevalcore, Finale Emilia e Mirandola). In più, è stato predisposto un team di psicologi per assistere i dipendenti colpiti dal lato lavorativo o da quello personale. Sono state organizzate tre sessioni d'aula, a cui hanno partecipato 60 persone per trattare disturbi traumatici da stress. In seguito, è stata la volta della seconda fase, durante la quale è stato effettuato un collegamento con la protezione civile e il gruppo di lavoro Abi Lab.

**D. Come è avvenuto il ritorno alla normalità?**

**R.** Gradualmente. Nel corso dei mesi, l'operatività bancaria è tornata in filiale, mentre i camper, i container e gli Atm mobili sono stati dismessi. Il processo di ritorno alla normalità si è chiuso venerdì 14 dicembre, giorno in cui l'ultima filiale colpita dal sisma è stata ripristinata. In tre casi, le dipendenze non sono state insediate negli stessi immobili in cui operavano in precedenza, ma all'interno di nuovi uffici.

**D. Che cosa ci può dire, invece, dei dati? La continuità operativa è stata assicurata?**

**R.** Il centro servizi non ha subito danni. I nostri sistemi di disaster recovery erano funzionanti, ma non ce n'è stato bisogno: abbiamo, infatti, attivato solo i processi di business continuity. Il nostro polo è ridondato tre volte: abbiamo un host che funziona normalmente e un altro che riparte se il primo non funziona: l'ultimo è quello di Cse, che riparte dopo quattro ore. Con il Consorzio servizi bancari abbiamo un supporto reciproco: se noi cadiamo, loro ci supportano. E viceversa. ■

**PRIMO LIVELLO**
**«Il sisma non ha danneggiato il nostro centro servizi», racconta Marco Bertazzoni, vicedirettore generale di Bper Services. «I nostri sistemi di disaster recovery erano funzionanti, ma non ce n'è stato bisogno: sono stati, infatti, attivati solo i processi di business continuity».**

**FILIALI DI EMERGENZA**
**La seconda scossa del terremoto di maggio ha danneggiato 20 filiali, che sono state sostituite, provvisoriamente, da camper, container e Atm mobili.**